UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE, et al., Plaintiffs, v. MICROSOFT CORPORATION, Defendant.	CASE NO. C20-1082JLR ORDER ON MICROSOFT'S MOTION FOR SUMMARY JUDGMENT

I. INTRODUCTION

Before the court is Defendant Microsoft Corporation's ("Microsoft") renewed motion for summary judgment. (Mot. (Dkt. # 127); Reply (Dkt. # 138).) Plaintiffs Steven Vance and Tim Janecyk (collectively, "Plaintiffs") oppose Microsoft's motion. (Resp. (Dkt. # 135[1]).) The court has considered the motion, all materials submitted in

[1] Plaintiffs originally filed their response under seal because it relied on and cited documents that Microsoft had marked confidential; they also filed a redacted version of their response. (Mot. to Seal (Dkt. # 134); Redacted Resp. (Dkt. # 132).) Because Microsoft did not oppose unsealing the response and the documents, the court denied Plaintiffs' motion to seal and

support of and in opposition to the motion, and the governing law. Being fully advised,[2] the court GRANTS Microsoft's motion for summary judgment.

II. BACKGROUND

The court sets forth the factual and procedural background of this case below.

A. Factual Background

1. The Diversity in Faces ("DIF") Dataset

Plaintiffs are longtime Illinois residents who, beginning in 2008, uploaded digital photographs, including photos of themselves, to Flickr, a photo-sharing website. (*See* Compl. (Dkt. # 1) ¶¶ 6-7, 28, 66-67, 75; Vance Dep.[3] at 9:15-10:9; Janecyk Dep.[4] at 39:7-40:1.) In 2014, Yahoo!, Flickr's then-parent company, publicly released a dataset of about 100 million photographs that had been uploaded to Flickr's website between 2004

---

directed the clerk to remove the seal on Plaintiffs' responsive brief and the confidential documents. (Mot. to Seal Resp. (Dkt. # 136); 7/11/22 Order (Dkt. # 137).) Accordingly, the court cites the unredacted version of Plaintiffs' response in this order.

[2] Both parties request oral argument on the motion (*see* Mot. at 1; Resp. at 1). The court, however, concludes that oral argument would not be helpful to its disposition of the motion. *See* Local Rules W.D. Wash. LCR 7(b)(4).

[3] Both parties have submitted excerpts from Mr. Vance's deposition. (*See* Berger Decl. (Dkt. # 86) ¶ 2, Ex. 1; 7/1/22 Lange Decl. (Dkt. # 132-1) ¶ 2, Ex. 1.) For ease of reference, the court cites directly to the page and line number of the deposition.

The court notes that Plaintiffs did not highlight the portions of the deposition transcripts that they referred to in their pleadings as required by Local Civil Rule 10(e)(10). *See* Local Rules W.D. Wash. LCR 10(e)(10) ("All exhibits [submitted in support of or in opposition to a motion] must be marked to designate testimony or evidence referred to in the parties' filings."). The court directs Plaintiffs' counsel to review the local rules regarding marking exhibits before making any further filings.

[4] Both parties have submitted excerpts from Mr. Janecyk's deposition. (*See* Berger Decl. ¶ 3, Ex. 2; 7/1/22 Lange Decl. ¶ 3, Ex. 2.) For ease of reference, the court cites directly to the page and line number of the deposition.

and 2014 (the "YFCC-100M Dataset"). (*See* Merler Decl. (Dkt. # 85) ¶ 3, Ex. A ("*Diversity in Faces*") at 2.) The YFCC-100M Dataset included photos uploaded by both Plaintiffs. (*See* Vance Dep. at 179:22-23; Janecyk Dep. at 95:22-24.)

Before 2018, "there was an industry-wide problem with many facial recognition systems' ability to accurately characterize individuals who were not male and did not have light colored skin tones." (Merler Decl. ¶ 4.) As a result, "the facial recognition systems and algorithms associated with those facial recognition systems were trained in such a way that the systems were able to accurately characterize a white, light skinned male subject, but the technology suffered from inaccuracies when it had to characterize a non-male or a person with darker skin tones." (*Id.*) Seeking to "advance the study of fairness and accuracy in face recognition technology," researchers working for International Business Machines Corporation ("IBM")[5] used one million of the photos in the YFCC-100M Dataset to develop the Diversity in Faces ("DiF") Dataset at issue in this case. (*Id.* ¶ 5; *Diversity in Faces* at 2, 7.) The researchers implemented ten "facial coding schemes" to measure aspects of the facial features of the individuals pictured in the photos, such as "craniofacial distances, areas and ratios, facial symmetry and contrast, skin color, age and gender predictions, subjective annotations, and pose and resolution." (*Diversity in Faces* at 9.) A statistical analysis of these coding schemes "provided insight into how various dimensions . . . provide indications of dataset diversity." (Merler

[5] All of the researchers involved in creating the DiF Dataset were based in and worked out of IBM's office in Yorktown Heights, New York; and the work was performed on and stored on IBM Research computer servers in Poughkeepsie, New York. (*Id.* ¶ 8.) None of the work involved computers or systems located in Illinois. (*Id.*)

Decl. ¶ 6.) The coding schemes implemented by the IBM researchers were intended to enable other researchers to develop techniques to estimate diversity in their own datasets, with the goal of mitigating dataset bias, and were "never intended to identify any particular individual." (*Id.* ¶ 7.) Rather, the coding schemes were "purely descriptive and designed to provide a mechanism to evaluate diversity in the dataset." (*Id.*)

IBM provided the DiF Dataset free of charge to researchers who filled out a questionnaire and submitted it to IBM via email. (*Id.* ¶¶ 4, 9.) The questionnaire required the researcher to verify

> (i) that he/she would only use the DiF Dataset for research purposes, and (ii) that he/she had read and agreed to the DiF Dataset terms of use, which made clear that the DiF Dataset could only be used for non-commercial, research purposes and prohibited using the DiF Dataset to identify any individuals in images associated with URLs in the DiF Dataset.

(*Id.* ¶ 9; *see also id.* ¶ 11, Ex. H (DiF Dataset terms of use).) After verifying that a request was for a "legitimate research purpose," IBM researcher Dr. Michele Merler sent the DiF Dataset to the requesting researcher "via an email that included a link to a temporary Box folder that contained the DiF Dataset." (Merler Decl. ¶ 10.)

2. Plaintiffs' Photos in the DiF Dataset

The DiF Dataset includes at least 61 of the nearly 19,000 public photos that Mr. Vance uploaded to Flickr. (Vance Dep. at 179:22-23, 210:19-24.) Mr. Vance appears in some of the photos in the DiF Dataset; other photos depict people whose state of residence was unknown to Mr. Vance and at least one depicts individuals who themselves were unknown to Mr. Vance. (*Id.* at 132:4-14; 154:5-16.)

The DiF Dataset includes 24 of the 1,669 public photos that Mr. Janecyk uploaded to Flickr. (Janecyk Dep. at 74:21-24, 95:22-96:1.) Mr. Janecyk appears in at least one of the photos. (*Id.* at 99:21-100:6.) Because Mr. Janecyk photographed people on the streets of Chicago, however, he does not know the names or places of residence of the individuals depicted in most of his photos. (*Id.* at 45:16-46:19, 98:8-100:13, 167:11-168:15, 228:19-21.)

3. Microsoft's Downloads of the DiF Dataset

Two individuals affiliated with Microsoft downloaded the DiF Dataset in February 2019: contractor Benjamin Skrainka and Microsoft Research intern Samira Samadi. (Skrainka Decl. (Dkt. # 87) ¶ 5; Samadi Decl. (Dkt. # 88) ¶¶ 5-6.) The court describes their interactions with the DiF Dataset below.

a. Benjamin Skrainka

Between September 7, 2018, and August 1, 2019, Mr. Skrainka worked as an independent contractor for Neal Analytics, LLC, a Washington-based consulting firm, through which he contracted as a vendor to Microsoft. (Skrainka Decl. ¶ 2; Skrainka Dep.[6] at 91:7-24, 111:8-23.) During this period, Mr. Skrainka provided support for a project, Azure Intelligent Storage ("AIS"), for Microsoft. (Skrainka Decl. ¶ 3.) His work related to defining a benchmark protocol for evaluating a third-party facial recognition technology that Microsoft was considering acquiring. (*Id.*; Kasap Decl. (Dkt. # 91)

[6] Both parties have submitted excerpts from Benjamin Skrainka's deposition. (*See* 5/19/22 Wiese Decl. (Dkt. # 129) ¶ 2, Ex. 1; 7/1/22 Lange Decl. ¶ 12, Ex. 11; 7/29/22 Wiese Decl. (Dkt. # 139) ¶ 2, Ex. 9.) For ease of reference, the court cites directly to the page and line number of the deposition.

¶¶ 2-3.) Mustafa Kasap, a Principal Program Manager, was Mr. Skrainka's manager and technical advisor for this project. (Skrainka Decl. ¶ 4; Kasap Decl. ¶ 2; Skrainka Dep. at 121:11-15.) As part of his project, Mr. Skrainka "determined what the parameters and/or methodology should be for comparing different face recognition technologies available in the market," including the technology that Microsoft considered acquiring, and developed code to implement these benchmarks. (Skrainka Decl. ¶ 3; Kasap Decl. ¶ 4.) He researched datasets containing photographs that might be suitable for making these comparisons. (Skrainka Decl. ¶ 4.)

On or about February 1, 2019, Mr. Skrainka requested a copy of the DiF Dataset from IBM. (Skrainka Decl. ¶ 4.) After Mr. Skrainka filled out IBM's questionnaire, IBM granted him access to the DiF Dataset through an online link. (Skrainka Decl. ¶ 5.) He downloaded the DiF Dataset sometime in early February 2019 while in Washington. (*Id.*) Mr. Skrainka evaluated the suitability of the photographs linked in the DiF Dataset for his project by manually inspecting some of the images and used some of the metadata in the DiF Dataset to "shrink or expand images to a consistent size" and to "extract the relevant faces" before running Microsoft's facial recognition software on them. (*Id.* ¶¶ 6-7; Skrainka Dep. at 229:18-230:21, 231:13-18, 233:15-235:6.) He was not interested in the coding schemes or facial annotations included in the DiF Dataset. (Skrainka Dep. at 227:21-229:23.) He determined that the images were not suitable for his benchmarking research because they "did not look like a conventional head-on photograph used on a driver's license or passport" and were of generally low quality. (Skrainka Decl. ¶ 7; *see also* Skrainka Dep. at 233:7-235:6 (explaining reasons the

images were not suitable).) Consequently, he did not further pursue using the DiF Dataset. (Skrainka Decl. ¶ 7.)

Mr. Skrainka was unaware that the DiF Dataset included any photographs or data related to Illinois residents. (*Id.* ¶ 12.) He did not share the DiF Dataset with anyone at Microsoft and is unaware of any other Microsoft group using the DiF Dataset, although he acknowledges that others could have accessed the dataset while it was stored in the cloud without his knowing. (*Id.*; Skrainka Dep. at 362:14-363:24; *see also* Kasap Decl. ¶ 7 (stating he, too, was unaware of any other Microsoft group using the DiF Dataset).)

Mr. Skrainka does not recall where, "if at all," he saved his copy of the DiF Dataset. (Skrainka Decl. ¶ 8.) During his project, however, Microsoft instructed him to use a virtual machine[7] for his work, and he recalled that "any facial-recognition-related work that [he] performed . . . was loaded only onto virtual machines and cloud storage in Azure." (*Id.*; Skrainka Dep. at 188:12-23.) When an Azure user creates a virtual machine or sets up "blob" storage, he or she is prompted to select an Azure Region that determines the geography of the data centers where the data will be stored; each Azure Region includes "availability zones" that map to specific datacenters within the selected region. (Kuttiyan Decl. (Dkt. # 128) ¶ 3.) Mr. Skrainka believes that he used a "West Coast availability zone" for the work that he performed and that he was "almost surely" using West Coast data centers "because they're faster." (Skrainka Dep. at 147:2-20,

[7] "A virtual machine emulates the characteristics of a stand-alone physical computer. It shares physical resources, such as servers, with other virtual machines, and each virtual machine is isolated by software." (*Id.*)

154:10-20.) He acknowledged, however, that he might have saved data in other availability zones, including the East Coast availability zone, and that he was unaware of whether the data was backed up or migrated to other availability zones. (Skrainka Dep. at 148:15-17, 151:19-24, 185:15-20; *see also* 7/1/22 Lange Decl. ¶ 19, Ex. 18 ("Kuttiyan Dep.") at 62:17-63:4, 63:24-65:2 (acknowledging that data may be backed up to data centers in other availability zones).) When his project ended, Mr. Skrainka decommissioned all virtual machines that he used in the project, including any data stored on those virtual machines or in the cloud. (Skrainka Decl. ¶ 8.)

Microsoft has been unable to confirm if and where on its systems Mr. Skrainka stored his copy of the DiF Dataset. (Mot. at 7; *see* Brunke Decl. (Dkt. # 92) ¶¶ 5-6.) In its July 15, 2021 supplemental answers to Plaintiffs' interrogatories, it stated that if Mr. Skrainka's copy of the DiF dataset had been stored on Microsoft servers in the cloud, the file would have been "chunked (i.e., divided into non-overlapping packets of data bits)" and encrypted, and the encrypted chunks would have been stored in data centers, likely in San Antonio, Texas and Chicago, Illinois. (Lange Decl. ¶ 20, Ex. 19 at 9-10 (supplemental answer to ROG No. 8).) In its second supplemental answers served after Mr. Skrainka's deposition, however, Microsoft "amend[ed] and correct[ed]" its supplemental answer to state that data stored on virtual machines and "blob" storage in the "West US" availability zone in February 2019 would have been stored in servers located in Washington or California, rather than in Illinois. (*Id.* at 10-11 (second supplemental answer to ROG No. 8); *see* Kuttiyan Decl. ¶ 4, Ex. A.)

b. Samira Samadi

Between January 22, 2019, and May 3, 2019, while she was a graduate student at Georgia Institute of Technology in Atlanta, Georgia, Ms. Samadi completed a student internship at Microsoft Research in New York City, New York. (Samadi Decl. ¶ 2.) The "focus of [her] internship was a research project involving the study of how humans interact with, use, and make decisions with facial recognition systems." (*Id.* ¶ 3.) She "wanted to design a controlled human-subject experiment where participants were shown examples of images of faces and asked to judge the similarities of the faces in the images given the similarity score generated by an automatic facial recognition system." (*Id.*) Her goal was "to measure how the humans' judgments of face similarities are affected by perceived race, skin tone, and gender of the faces they are shown." (*Id.*) Her research was not focused on identifying people through facial recognition systems and did not involve measuring facial geometry or features. (*Id.* ¶ 4.) Ms. Samadi's research was supervised by Microsoft Senior Principal Researcher Jenn Wortman Vaughan, who was also based in New York. (Vaughan Decl. (Dkt. # 89) ¶¶ 1, 3.)

To run her experiment, Ms. Samadi needed "multiple photographs of the same individual, all of which needed to be directly facing the camera or slightly angled." (Samadi Decl. ¶ 4.) On or about February 20, 2019, she asked IBM for access to the DiF Dataset using her Georgia Institute of Technology credentials. (*Id.* ¶ 5, Ex. A (email requesting access); *see also* Vaughan Decl. ¶ 7, Ex. B (email thread discussing Ms. Samadi's request for the DiF Dataset).) IBM directed Ms. Samadi to fill out its questionnaire, and after she did so, granted her access to the DiF Dataset through an

online link. (Samadi Decl. ¶ 6.) She downloaded the dataset on or about February 25, 2019, while working at Microsoft Research in New York. (*Id.*)

After she downloaded the DiF Dataset, Ms. Samadi "briefly reviewed" some of the photographs linked in that dataset. (*Id.* ¶ 7; *see also* Samadi Dep.[8] at 20:5-7 (stating she reviewed the DiF Dataset for about half an hour).) She determined that the photos were not suitable for her project because there were not multiple photos of the same individual facing the camera. (Samadi Decl. ¶ 7.) She did not further review the images in the DiF Dataset. (*Id.*; *see also id.*, Ex. C (email to Dr. Vaughan, stating that after "looking closely" at the "IBM data," she found that it did not have multiple images for one person and that the images have "many different backgrounds").) She did not use the DiF Dataset in her project and the DiF Dataset did not play any role in the development of the paper that she wrote with Dr. Vaughan about the results of her research. (*Id.* ¶ 11, Ex. E (research paper); Vaughan Decl. ¶¶ 7-8.)

Ms. Samadi was "not aware of or interested in any facial annotations" in the DiF Dataset, did not review any such data, and did not share the link to download the DiF Dataset with anyone else. (Samadi Decl. ¶ 8.) She did not know that the DiF Dataset included photographs or data relating to Illinois residents. (*Id.* ¶ 9.) Neither Ms. Samadi nor Dr. Vaughn are aware of any other projects at Microsoft Research that used the DiF

[8] Both parties have submitted excerpts from Samira Samadi's deposition. (*See* 5/19/22 Wiese Decl. (Dkt. # 129) ¶ 3, Ex. 2; 7/1/22 Lange Decl. ¶ 22, Ex. 21.) For ease of reference, the court cites directly to the page and line number of the deposition.

Dataset, nor are they aware of the DiF Dataset being used by any other group at Microsoft. (*Id.* ¶ 12; Vaughan Decl. ¶ 11.)

Ms. Samadi believes, but is not certain, that she downloaded the DiF Dataset to her Microsoft Research laptop. (Samadi Decl. ¶ 6; Samadi Dep. at 38:20-39:6.) Under Microsoft's Data Retention and Disposal Standard, data saved on Ms. Samadi's Microsoft Research laptop was deleted within 180 days of the end of her internship. (Swann Decl. (Dkt. # 90) ¶ 9.) It is possible, however, that Ms. Samadi may have saved the DiF Dataset to her OneDrive account[9] or that her laptop was automatically uploading information to OneDrive. (*See* Chirico Decl. (Dkt. # 93) ¶ 2, Ex. A[10] ("3/11/19 Samadi Email") (email from Ms. Samadi to Mr. Chirico, in which she states that she works with and must download "big data sets" and that her OneDrive account was full); Samadi Dep. at 65:6-20, 57:1-19; Lange Decl. ¶ 20, Ex. 19 at 9 (supplemental answer to ROG No. 8) (stating that Microsoft's investigation "has not established how Ms. Samadi initially downloaded or stored the IBM DiF Dataset").) If Ms. Samadi's copy of the DiF dataset was saved to Ms. Samadi's OneDrive account, the file would have been "chunked (i.e., divided into non-overlapping packets of data bits) and encrypted, and the encrypted chunks would have been stored in [Microsoft's] data centers, likely in San Antonio, Texas and Chicago, Illinois." (Lange Decl. ¶ 20, Ex. 19 at 10-11 (second supplemental answer to ROG No. 8).)

[9] OneDrive is Microsoft's cloud file hosting and storage service. (Swann Decl. ¶ 4.) It allows Microsoft personnel to store their files and data in the cloud. (*Id.*)

[10] Plaintiffs also provided this email thread as an exhibit. (*See* Lange Decl. ¶ 25, Ex. 24.)

In March 2019, Ms. Samadi reached out to Jeff Chirico, who provided information technology support for Microsoft Research in New York, to ask where she should store data related to her research project. (3/11/19 Samadi Email; Samadi Dep. at 50:24-51:12; Chirico Decl. ¶¶ 1-2.) Mr. Chirico instructed her to save her data on a "hidden share" on a Microsoft Research server located in New York. (3/11/19 Samadi Email; Chirico Decl. ¶¶ 2-3.) This server is not backed up to any other server, and access to the server is restricted to Microsoft Research. (Chirico Decl. ¶ 3.) Microsoft later found a copy of the DiF Dataset and other data from Ms. Samadi's internship on the Microsoft Research server in New York. (Lange Decl. ¶ 20, Ex. 19 at 8 (answer to ROG No. 8).)

B. Relevant Procedural Background

Plaintiffs filed their proposed class complaint in this action on July 14, 2020. (Compl.) They brought claims against Microsoft for violations of two provisions of Illinois's Biometric Information Privacy Act, 740 ILCS § 14/1, *et seq.* ("BIPA"), unjust enrichment, and injunctive relief. (*Id.* ¶¶ 93-122.) With respect to the BIPA violations, Plaintiffs alleged that Microsoft (1) violated BIPA § 15(b) by collecting and obtaining their biometric data without providing required information or obtaining written releases, and (2) violated BIPA § 15(c) by unlawfully profiting from Plaintiffs' biometric data. (*Id.* ¶¶ 93-106.)

On September 14, 2020, Microsoft moved to dismiss Plaintiffs' claims. (MTD (Dkt. # 25).) On March 15, 2021, the court granted in part and denied in part Microsoft's motion to dismiss. (3/15/21 Order (Dkt. # 43).) The court (1) granted Microsoft's motion to dismiss Plaintiffs' injunctive relief claim on the ground that injunctive relief is

not a standalone cause of action; (2) denied Microsoft's motion to dismiss Plaintiffs' BIPA § 15(b) claim, concluding that Plaintiffs had sufficiently alleged the elements of the claim; and (3) deferred ruling on Microsoft's motion to dismiss Plaintiffs' BIPA § 15(c) and unjust enrichment claims pending the receipt of supplemental briefing. (*See generally id.*) On April 14, 2021, after reviewing the parties' supplemental briefing and hearing oral argument, the court dismissed Plaintiffs' BIPA § 15(c) claim with leave to amend and denied Microsoft's motion to dismiss Plaintiffs' unjust enrichment claim. (*See* 4/13/21 Min. Entry (Dkt. # 46); 4/14/21 Order (Dkt. # 47).) Despite being granted leave to do so, Plaintiffs did not amend their BIPA § 15(c) claim. (*See generally* Dkt.)

Microsoft filed its original motion for summary judgment on December 10, 2021. (1st MSJ (Dkt. # 84).) On February 8, 2022, the court granted in part Plaintiffs' motion for additional discovery pursuant to Federal Rule of Civil Procedure 56(d) and struck Microsoft's original motion for summary judgment without prejudice. (2/8/22 Order (Dkt. # 118); *see also* Pls. 56(d) Mot. (Dkt. # 107).)

On May 19, 2022, Microsoft filed the instant renewed motion for summary judgment. (*See* Mot.) Subsequently, the parties agreed to a stipulated briefing schedule to allow Plaintiffs to obtain additional discovery. (5/27/22 Stip. (Dkt. # 130).) Thus, this motion became ripe for decision on July 29, 2022. (*Id.*)

III. ANALYSIS

Microsoft argues that summary judgment on Plaintiffs' claims is warranted because (1) BIPA cannot apply extraterritorially to its conduct outside of Illinois as a matter of Illinois law; (2) applying BIPA to Microsoft's conduct would violate the

dormant Commerce Clause of the United States Constitution; (3) even if BIPA could apply to Microsoft's out-of-state conduct, Plaintiffs cannot prove the elements of their BIPA § 15(b) claim; and (4) Plaintiffs cannot prove the elements of their unjust enrichment claim. (*See generally* Mot.) Below, the court sets forth the standard for evaluating motions for summary judgment before considering Microsoft's motion.

A. Summary Judgment Standard

Under Rule 56 of the Federal Rules of Civil Procedure, either "party may move for summary judgment, identifying each claim or defense—or the part of each claim or defense—on which summary judgment is sought." Fed. R. Civ. P. 56. Summary judgment is appropriate if the evidence, when viewed in the light most favorable to the non-moving party, demonstrates "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." *Id.*; *see Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). A dispute is "genuine" if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A fact is "material" if it "might affect the outcome of the suit under the governing law." *Id.*

The moving party bears the initial burden of showing that there is no genuine dispute of material fact and that it is entitled to prevail as a matter of law. *Celotex*, 477 U.S. at 323. If the moving party does not bear the ultimate burden of persuasion at trial, it nevertheless "has both the initial burden of production and the ultimate burden of persuasion on a motion for summary judgment." *Nissan Fire & Marine Ins. Co. v. Fritz Companies, Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000). "In order to carry its burden of

production, the moving party must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial." *Id.* If the moving party meets its burden of production, the burden then shifts to the nonmoving party to identify specific facts from which a factfinder could reasonably find in the nonmoving party's favor. *Celotex*, 477 U.S. at 324; *Anderson*, 477 U.S. at 250.

The court is "required to view the facts and draw reasonable inferences in the light most favorable to the [nonmoving] party." *Scott v. Harris*, 550 U.S. 372, 378 (2007). The court may not weigh evidence or make credibility determinations in analyzing a motion for summary judgment because these are "jury functions, not those of a judge." *Anderson*, 477 U.S. at 249-50. Nevertheless, the nonmoving party "must do more than simply show that there is some metaphysical doubt as to the material facts . . . . Where the record taken as a whole could not lead a rational trier of fact to find for the nonmoving party, there is no genuine issue for trial." *Scott*, 550 U.S. at 380 (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986) (internal quotation marks omitted)).

B. Extraterritoriality Doctrine

Under Illinois law, a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005) (quoting *Dur-Ite Co. v. Indus. Comm'n*, 68 N.E.2d 717 (Ill. 1946) (internal quotation marks omitted)). Because BIPA does not

contain such an express provision, it does not apply extraterritorially to conduct outside of Illinois. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017); (*see* 3/15/21 Order at 6). Thus, to survive summary judgment, Plaintiffs must show a genuine issue of material fact regarding whether the circumstances underlying their BIPA claims "occurred primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854; (*see also* 3/15/21 Order at 6).

Microsoft asserts that Illinois's extraterritoriality doctrine bars Plaintiffs' BIPA claims because none of its conduct relating to those claims took place in Illinois. (Mot. at 11-15.) Rather, its relevant conduct—downloading, reviewing, and evaluating the DiF Dataset—took place in Washington and New York. (*Id.* at 13-15.) Thus, according to Microsoft, Plaintiffs cannot prove that its conduct "occurred primarily and substantially in Illinois." (*Id.* at 10-11 (citing *Avery*, 835 N.E.2d at 854).) Plaintiffs, for their part, counter that the extraterritoriality doctrine does not apply because Microsoft's relevant conduct occurred in Illinois. (Resp. at 10-16.) The court agrees with Microsoft that the extraterritoriality doctrine bars Plaintiffs' BIPA claims as a matter of law.

Plaintiffs have not met their burden at summary judgment to establish a genuine issue of material fact regarding whether Microsoft's relevant conduct "occurred primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854. First, Plaintiffs rely on the court's order denying Microsoft's motion to dismiss, in which the court identified the allegations in Plaintiffs' complaint that precluded dismissal on extraterritoriality grounds. (Resp. at 13-14 (quoting 3/15/21 Order at 8).) At summary judgment, however, Plaintiffs can no longer rest on their allegations. Instead, they must identify evidence sufficient to

establish a genuine issue of material fact regarding whether the circumstances giving rise to their claims occurred "primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854. As discussed below, they have not met this burden.

Second, Plaintiffs contend that the extraterritoriality doctrine does not bar their claims because (1) Plaintiffs resided in Illinois; (2) Plaintiffs' photos from which their biometric data was collected were taken in Illinois and uploaded to the Internet in Illinois; and (3) Plaintiffs' injuries occurred in Illinois. (Resp. at 14-15.) They also contend that "both Mr. Skrainka and Ms. Samadi likely downloaded the [DiF D]ataset to a datacenter in Illinois." (*Id.* at 11-12.) At most, however, they point to the possibility that Microsoft may have stored "chunked" and encrypted copies of the DiF Dataset on a cloud server located in Illinois. (*Id.*; Lange Decl. ¶ 20, Ex. 19 at 9-11.) But as Microsoft points out, even if Plaintiffs could prove that Microsoft stored the DiF Dataset in a datacenter in Illinois, the relevant section of BIPA regulates only the acquisition of data, rather than the encrypted storage of data after it is acquired. (Mot. at 13); 740 ILCS § 14/15(b) (stating that "[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information"). Plaintiffs have not identified any other relevant conduct by Microsoft that took place either primarily or substantially in Illinois. (*See generally id.*)

The cases Plaintiffs cite in support of their argument that claims "relating to photos taken and uploaded to the internet in Illinois" necessarily survive the extraterritoriality doctrine are all distinguishable from the present case. (*See* Resp. at 14-16.) In *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547 (N.D. Cal.

2018), for example, the plaintiff Illinois residents uploaded their photos to Facebook's social media service in Illinois. Facebook then scanned the photos, identified the individuals in those photos, and suggested names of individuals to tag in those photos. *Id.* Thus, Facebook reached into Illinois by providing its service to the plaintiffs, and the plaintiffs' direct interactions with Facebook gave rise to the alleged BIPA violations. *See id.* (noting that Facebook had not "tendered any evidence" that the circumstances relating to its conduct did not occur "primarily and substantially within" Illinois); *id.* at 549 (granting the plaintiffs' motion for class certification).

Plaintiffs' remaining citations are to decisions denying motions to dismiss. (*See* Resp. at 14-15.) In *In re Clearview AI, Inc. Consumer Privacy Litig.*, 585 F. Supp. 3d 1111, 1118, 1121 (N.D. Ill. 2022), *clarified on denial of reconsideration by* 2022 WL 2915627 (N.D. Ill. July 25, 2022), the court observed, in denying the defendants' motion to dismiss on extraterritoriality grounds, that the plaintiffs had alleged that the defendants "trespassed on the Illinois subclass members' private domains in Illinois," "contracted with hundreds of Illinois entities, both public and private," and "used artificial intelligence algorithms to scan the face geometry of each individual depicted to harvest the individuals' unique biometric identifiers." *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017), involved a challenge to Google's alleged practice of automatically uploading photos taken by Illinois residents on Google Droid devices in Illinois to its Google Photos service; immediately scanning the photos to create "templates" that mapped the Illinois plaintiffs' "distinct facial measurements"; and then using those templates to "find and group together other photos of" the Illinois plaintiffs.

Similarly, in *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017), the Illinois plaintiff alleged that when he uploaded a photo to Shutterfly's website, Shutterfly's facial recognition software scanned the image, located the faces in the image, and extracted a template for each face that could be used to identify the persons in the photo. In all of these cases, the plaintiffs alleged that the defendant itself reached into Illinois to collect their photographs, scan the photographs, and/or generate facial measurements or templates for use in facial recognition systems without the plaintiffs' consent.

Here, in contrast, there is no dispute that other entities—rather than Microsoft—were responsible for the collection of the photographs, the scanning of the photographs, and the generation of facial measurements or templates. (*See* Mot. at 3-4 (describing the conduct of Flickr, Yahoo, and IBM in collecting photos, creating datasets, and generating facial measurements); Resp. at 3-10 (describing Microsoft's conduct in downloading and evaluating the DiF dataset); *see generally id.* (making no argument disputing Microsoft's description of Flickr, Yahoo, and IBM's conduct).) Furthermore, Plaintiffs identify no evidence that either Mr. Skrainka or Ms. Samadi had any relevant connection to Illinois (aside from the possibility that Microsoft saved their data in a data center in Illinois), let alone downloaded, reviewed, or evaluated the DiF Dataset in Illinois. (*See generally* Resp.) As a result, this case is closer in nature to *McGoveran v. Amazon Web Services, Inc.*, C.A. No. 20-13399-LPS, 2021 WL 4502089, at *4 (D. Del. Sept. 30, 2021), in which the court noted that the plaintiffs' allegations about the case's connections to Illinois were "nothing more than repeated statements (phrased three different ways) about

Plaintiffs' residency" and granted the defendant's motion to dismiss under the extraterritoriality doctrine.

The court concludes that, even if Microsoft's systems "chunked," encrypted, and stored the DiF Dataset on a server in Illinois, any connection between Microsoft's conduct and Illinois is too attenuated and *de minimis* for a reasonable juror to find that the circumstances underlying Microsoft's alleged BIPA violation "occurred primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854; *see also McGoveran*, 2021 WL 4502089, at *4-6. Therefore, the court GRANTS Microsoft's motion for summary judgment on Plaintiffs' BIPA claim.[11]

B. Unjust Enrichment

To prevail on a claim for unjust enrichment under Illinois law,[12] a plaintiff must prove (1) that the defendant has unjustly retained a benefit to the plaintiff's detriment and (2) that the defendant's retention of the benefit "violates the fundamental principles of justice, equity, and good conscience." *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 545 N.E.2d 672, 679 (Ill. 1989). Plaintiffs alleged that Microsoft "obtained a monetary benefit from Plaintiffs . . . to their detriment . . . by profiting off of

[11] Because the court grants Microsoft's motion for summary judgment on extraterritoriality grounds, it need not address Microsoft's argument that the extraterritorial application of BIPA in this case would violate the Dormant Commerce Clause or Microsoft's specific arguments relating to BIPA § 15(b).

[12] The court previously determined that Illinois law governed Plaintiffs' unjust enrichment claim. (4/14/21 Order at 20-21.)

Plaintiffs' . . . biometric identifiers and information" without providing "full compensation for the benefit received from Plaintiffs." (Compl. ¶¶ 108, 111.)

Microsoft asserts that it is entitled to summary judgment on Plaintiffs' unjust enrichment claim because it "did not use the DiF Dataset at all" and therefore "could not possibly have obtained any 'monetary benefit' or 'profit' from Plaintiffs' biometric identifiers or information." (Mot. at 23-24.) Rather, according to Microsoft, Mr. Skrainka and Ms. Samadi "each reviewed some linked photos briefly, but neither they nor anyone else at Microsoft used the DiF Dataset for any purpose—much less used the annotations that Plaintiffs claim are biometrics." (Mot. at 24.) Plaintiffs counter that summary judgment is precluded because there is a material question of fact as to whether Microsoft profited from its use of the DiF Dataset. (Resp. at 24.) Specifically, they contend that Mr. Skrainka[13] downloaded the DiF Dataset to evaluate a facial recognition product that Microsoft was considering purchasing and that there is a question of fact as to whether Mr. Skrainka in fact used the DiF Dataset or some other dataset to accomplish that work. (*Id.* (citing Skrainka Dep. at 356:4-22, 340:19-341:3).) In reply, Microsoft asserts that it is undisputed that Mr. Skrainka never used the facial annotations in the DiF Dataset—rather, his evaluation used only the Flickr URLs for the photos, a sample of photos, and spatial coordinates locating faces within a photo, none of which constitute biometric identifiers or information. (Reply at 12 (citing 740 ILCS § 14/10 ("'Biometric

[13] Plaintiffs make no argument that Ms. Samadi's conduct forms the basis of any unjust enrichment claim. (*See* Resp. at 24.)

identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include . . . photographs . . . .").)

Viewing the evidence in the light most favorable to Plaintiffs, the court concludes Plaintiffs have not met their burden to identify specific facts from which a jury could reasonably find that Microsoft unjustly retained a benefit to Plaintiffs' detriment. To the contrary, the court agrees with Microsoft that Plaintiffs have presented no evidence that would establish a genuine issue of fact regarding whether Microsoft used Plaintiffs' biometric information or identifiers to its benefit, much less that Microsoft obtained some sort of monetary benefit from their biometric information. Accordingly, the court GRANTS Microsoft's motion for summary judgment on Plaintiffs' unjust enrichment claim.[14]

IV. CONCLUSION

For the foregoing reasons, the court GRANTS Microsoft's motion for summary judgment (Dkt. # 127).

Dated this 17th day of October, 2022.

JAMES L. ROBART
United States District Judge

[14] For the same reasons, the court concludes that the result would be the same if Washington law applied to Plaintiffs' unjust enrichment claim. *See Cousineau v. Microsoft*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012) (setting forth the elements of an unjust enrichment claim under Washington law).